CHAPTER

5

INSTALLING ACTIVE DIRECTORY

After completing this chapter, you will be able to:

- Create a Windows 2000 domain
- Understand the role of DCPromo.exe and the Configure Your Server wizard
- Use the Active Directory Installation Wizard
- Promote a member server to a domain controller
- Demote a domain controller to a member server
- Understand the role of the Active Directory database
- Understand the role of the shared system volume
- Understand Active Directory domain modes
- Install Active Directory on a Windows 2000 server
- Add additional domain controllers to a domain
- Change the mode of a Windows 2000 domain

This chapter discusses installing and configuring the Windows 2000 Active Directory. We will discuss the various tools available for installing Active Directory, the components of Active Directory that are installed, and the different domain modes that Active Directory supports. Through examples and projects, you will learn how to create Windows 2000 domains, manipulate domain controllers, and remove domains from the network.

As mentioned in an earlier chapter, the Windows 2000 Active Directory uses domain controllers (DCs) to store the database of objects and containers that create the domain tree. Each DC contains the complete records of that domain's objects, containers, and organizational units. Each of these DCs is a **peer**, meaning that it is capable of providing domain logon, security, and management functionality.

When we speak of installing Active Directory, we really mean installing the Active Directory service on the DCs themselves. Many Windows 2000 servers are installed as member servers of a domain, and although they participate in the domain, they are not running Active Directory service itself. Rather, the member servers are Active Directory clients.

Note

Member servers can be upgraded to DCs, and DCs can be demoted to member servers. This is a significant change from Windows NT 4 and earlier. We will discuss changing the role of a server later in this chapter.

Before we launch into a discussion of the actual installation of Active Directory within a Windows 2000 environment, we first need to discuss some preinstallation issues. Although some of this material will be a review of previous chapters, the importance of planning the initial installation of Active Directory cannot be overemphasized.

Preparing for Active Directory Installation

It is extremely tempting to jump into Windows 2000 at full speed. In fact, the initial installation almost encourages that approach, with the Configure Your Server wizard launching immediately after the first installation. If you accept all the defaults while installing the first DC, however, the resulting configuration may not be suitable for your environment. For example, the default initial installation will configure your server to run on the 10.x.x.x network with a 255.0.0.0 subnet mask; it will also install the Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) services on the server. This configuration probably will not match your company's needs. Although the server can be reconfigured later, it is more efficient and effective to configure it correctly the first time.

Preparing IP Addressing Schemes and DNS

Unless you are creating a network from scratch or migrating from another network protocol, your environment probably has an existing TCP/IP addressing scheme and naming convention. Your naming convention is likely to be a NetBIOS naming style, with server names like Exchange01 and FileSrv01 or even Hermes. Although Windows 2000 servers provide backward compatibility with NetBIOS naming, a native Windows 2000 network environment operates entirely upon a DNS name resolution.

Domain Context

Unlike previous versions of Windows NT, a Windows 2000 domain does not stand alone. Instead, every domain exists within a **context**, or relationship, with every other domain in a domain tree. Windows 2000 automatically creates the required two-way and transitive trusts required to allow the newly created domain to function within the tree. During installation of the first DC, the Active Directory Installation Wizard uses the provided information to install the DC and create the domain within the existing context of other domains and DCs. If no other domains exist, then the newly created domain functions as the root domain.

Your planning will determine the context in which the new domain should be installed. For some network environments, organizing and installing domains along business lines will be appropriate. For others, a geographical breakdown makes much more sense. As an example, let us look at a fictional company and some ways to organize its domain tree.

Texas Pinball and Cattle Co. is a company that specializes in the sale and service of pinball machines to home and business markets. This company has offices scattered around Texas, but primarily it focuses in the Dallas/Fort Worth, Houston, and San Antonio markets. Each market has a home office and branch offices. Each office both sells and supports pinball machines.

Assuming that the company needs multiple domains, there are several ways to divide the organization. First, let's look at a geographical split. The company can be broken into a northern region that encompasses the Dallas/Fort Worth area and a southern region that encompasses San Antonio and Houston. For our purposes, we will call these the North region and the South region. If TexasPinball.com is the root domain owned by the Texas Pinball and Cattle Co., then each region could have a child domain: North.TexasPinball.com and South.TexasPinball.com. Naturally, these domains could be broken down even further by cities, if needed. The resulting structure would look something like Figure 5-1.

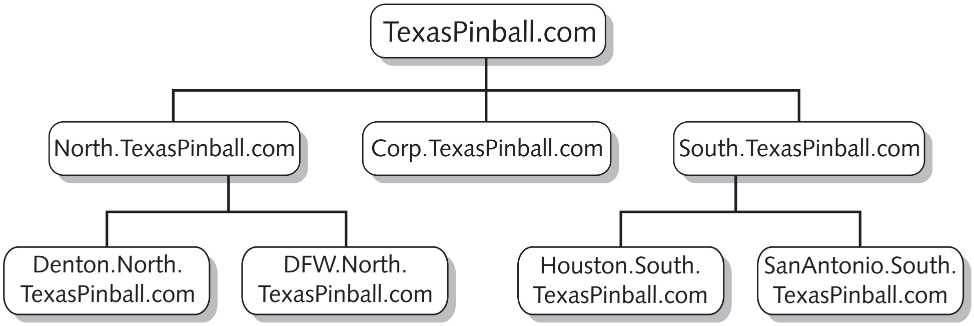


Figure 5-1 Geographical domain organization

Another method of organization is to split along business divisions. Once again, assuming that the company needs multiple domains, a natural division exists between the Sales and the Service departments. For our purposes, we will call these the Sales division and the Service division. If TexasPinball.com is the root domain owned by the Texas Pinball and Cattle Co., then each division could have a child domain: Sales.TexasPinball.com and Service.TexasPinball.com. Naturally, these domains could be broken down further if necessary—for example, home and business sales, electromechanical, and solid-state repairs. The resulting structure could look something like Figure 5-2.

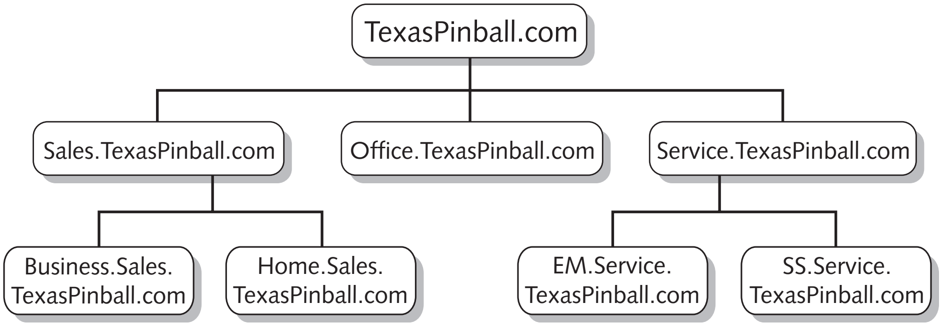


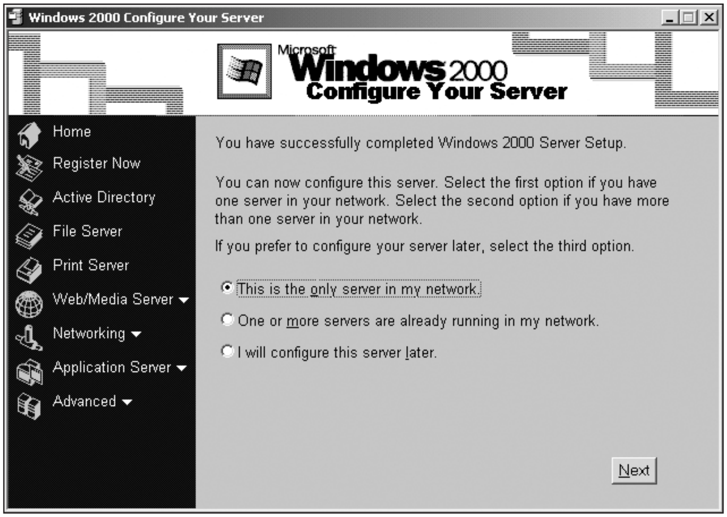
Figure 5-2 Business model domain organization

INSTALLING ACTIVE DIRECTORY

Once the planning for the Active Directory is finished, it is time to move on to the actual installation. Windows 2000 uses guides called **wizards** to perform many of the administrative and configuration tasks. The Active Directory service is installed using one of these wizards. The Active Directory Installation Wizard can be used to install Active Directory, upgrade a member server to a DC, or demote a DC to a member server. You can use two methods to launch the wizard—the Configure Your Server wizard and a program named dcpromo.exe—depending upon whether the server is newly built or has been previously configured. We will be looking at both of these methods and how to use them in this section.

Configure Your Server

If the server is newly built, a configuration wizard will follow the initial installation. This Configure Your Server wizard will allow you to install Active Directory on a server and configure it as the initial server in a domain. As mentioned earlier, the default configuration will result in a server running on the 10.x.x.x network with a 255.0.0.0 subnet mask and will also install the DHCP and DNS services on the server. Naturally, you can adjust each of these elements to meet your needs; for many administrators, however, canceling the initial configuration wizard and later configuring only the needed services will be the most appropriate choice, as displayed in Figure 5-3.



You have successfully completed Windows 2000 Server Setup.

You can now configure this server. Select the first option if you have one server in your network. Select the second option if you have more than one server in your network.

If you prefer to configure your server later, select the third option.

● This is the only server in my network.

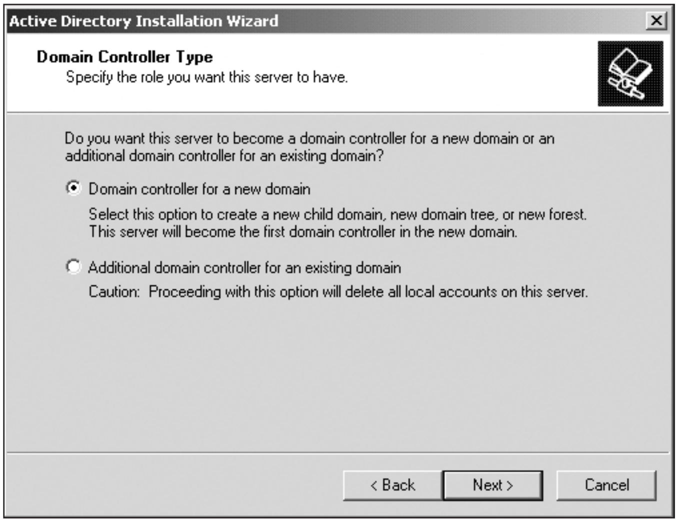
○ One or more servers are already running in my network.

○ I will configure this server later.

Figure 5-3 Initial Configure Your Server wizard

Dcpromo.exe

The Active Directory service can also be installed on a server that has been previously configured as a member server. The Active Directory Installation Wizard is activated via the dcpromo.exe program. To start the wizard, select Start|Run and enter "dcpromo.exe". The wizard will detect that Active Directory is not installed and will prompt whether to install the server as a domain controller in a new domain or as a new controller within an existing domain, as seen in Figure 5-4.



Domain Controller Type

Specify the role you want this server to have.

Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?

● Domain controller for a new domain

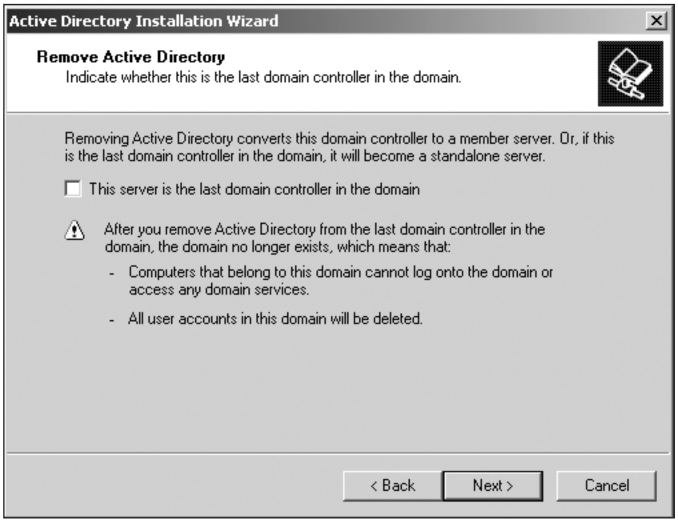
Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.

○ Additional domain controller for an existing domain

Caution: Proceeding with this option will delete all local accounts on this server.

Figure 5-4 Installing Active Directory with dcpromo.exe

You also use dcpromo.exe to remove the Active Directory service from a DC and demote it to a member server. As you can see in Figure 5-5, the wizard detects the DC status of the server. If the server is a DC, the only option presented is to demote the server to a member server status.



Active Directory Installation Wizard

Remove Active Directory
Indicate whether this is the last domain controller in the domain.

Removing Active Directory converts this domain controller to a member server. Or, if this is the last domain controller in the domain, it will become a standalone server.

□ This server is the last domain controller in the domain

After you remove Active Directory from the last domain controller in the domain, the domain no longer exists, which means that:

- Computers that belong to this domain cannot log onto the domain or access any domain services.
- All user accounts in this domain will be deleted.

Figure 5-5 Demoting a DC with dcpromo.exe

Note

If the last DC in a domain is demoted, the domain itself is destroyed and removed from the network. All domain user accounts and services are also removed.

In most cases, dcpromo.exe is the method you should use to invoke the Active Directory Installation Wizard. You should use the initial Configure Your Server wizard only when installing the first DC within a domain—and even then, the best technique is to configure any prerequisite services manually and then use dcpromo.exe to install the Active Directory services.

CREATING WINDOWS 2000 DOMAINS

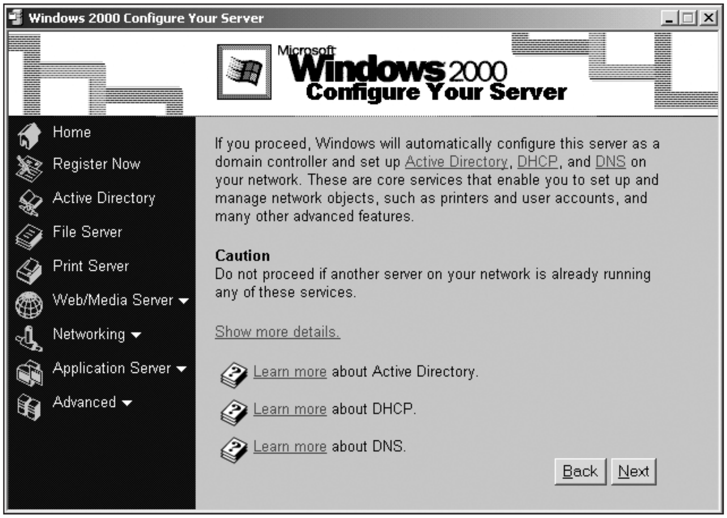
According to Microsoft, a Windows 2000 **domain** is a selection of computers or resources that share a single security boundary. In other words, everything within a domain shares the same security settings, rights, and relationships. Domains are not necessarily related to a geographical boundary; in fact, many companies have domains that consist of multiple physical locations. Conversely, multiple domains can serve a single physical location.

When multiple domains are interconnected via trust relationships, the domains can form a domain tree. A **domain tree** shares a common schema, Global Catalog, and contiguous namespace. Domains within a domain tree automatically form trust relationships that allow network resources to be shared throughout the tree. If several domain trees share a common schema, configuration, and Global Catalog, but do not share a contiguous namespace, then the trees are considered to form a **forest**.

Installing the Active Directory service on at least one DC forms a Windows 2000 domain. As mentioned earlier in this chapter, the Active Directory Installation Wizard can be invoked either through the initial Configure Your Server wizard or through dcpromo.exe, depending upon your needs and whether the Active Directory service has been previously configured on the server. In the next section, we will look at using the wizard to create a Windows 2000 domain, add an additional DC to the domain, and remove a DC from the domain.

USING THE ACTIVE DIRECTORY WIZARDS

After Windows 2000 is installed, the first screen presented to an administrator on the initial login is a Configure Your Server wizard, as seen in Figure 5-6. Due to the importance of the Active Directory service to a Windows 2000 network environment, that service is the first one presented by the configuration wizard.



If you proceed, Windows will automatically configure this server as a domain controller and set up Active Directory, DHCP, and DNS on your network. These are core services that enable you to set up and manage network objects, such as printers and user accounts, and many other advanced features.

Caution
Do not proceed if another server on your network is already running any of these services.

Show more details.

Learn more about Active Directory.

Learn more about DHCP.

Learn more about DNS.

Figure 5-6 The Configure Your Server wizard

Installing the First Domain

In this section, we will look at the default installation of the first Windows 2000 domain on a network. For the purposes of this section, we will install Active Directory on the server as if it were the first and only server on the network. This process will install the

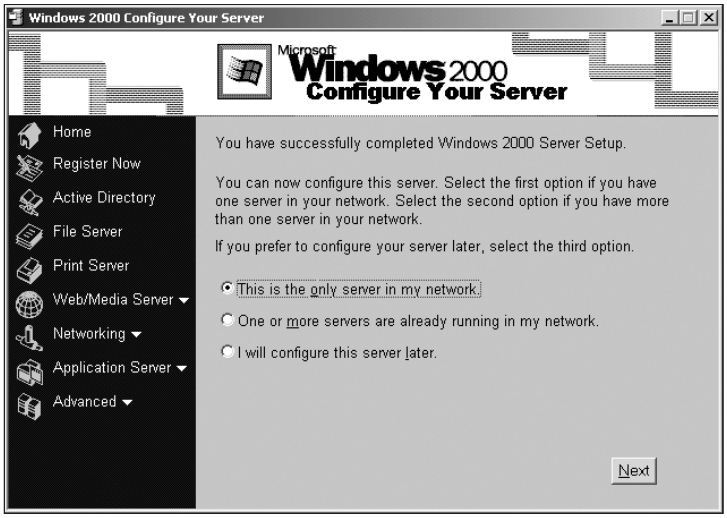
DHCP and DNS services in addition to the Active Directory service. In most real-world scenarios, some or all of these additional services will already be present within the network environment. If these services are already present, then Active Directory will need to be installed separately using the dcpromo program.

Beginning the Wizard

The Active Directory installation starts with the Configure Your Server wizard. After the initial installation of Windows 2000, this wizard walks you through the main configuration elements. The Configure Your Server wizard allows you to choose several different options, based on the role of the server within the network and whether an existing domain is already present (as was shown in Figure 5-4).

Installing the Domain

To install the first domain of a domain tree, first select the This Is The Only Server In My Network option from the opening screen in the wizard, and then click on the Next button as shown in Figure 5-7. The Active Directory Installation Wizard will automatically configure the server as a DNS and DCHP server, and it will also configure the server as a DC for the new domain. The wizard will inform you of these options, and it will also allow you to check the help files if you have any questions about the services it installs.



You have successfully completed Windows 2000 Server Setup.

You can now configure this server. Select the first option if you have one server in your network. Select the second option if you have more than one server in your network.

If you prefer to configure your server later, select the third option.

● This is the only server in my network.

○ One or more servers are already running in my network.

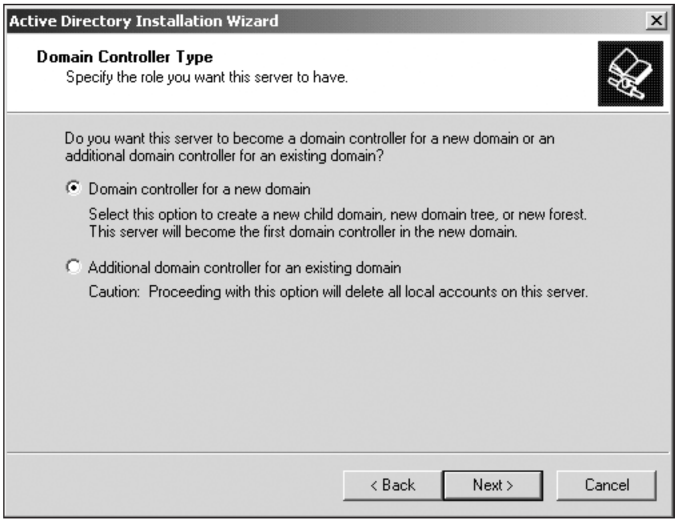
○ I will configure this server later.

Figure 5-7 Beginning configuration with the Configure Your Server wizard

Note: If DNS and DHCP services are already available on your network, the default configuration of the Configure Your Server wizard is likely to cause issues. You may wish to cancel from this wizard and use the DCPromo.exe utility as an alternative.

Role of the Domain Controller

When a server is promoted to a domain controller and the Active Directory service is installed on it, the Active Directory Installation Wizard will prompt for the role of the DC. The DC can be installed as the first DC in a new domain or as an additional controller within an existing domain. For our purposes, we wish to install this computer as the first DC within a new domain. To create a new domain, select Domain Controller For A New Domain, as shown in Figure 5-8, when prompted by the wizard.



Active Directory Installation Wizard

Domain Controller Type
Specify the role you want this server to have.

Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?

● Domain controller for a new domain

Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.

○ Additional domain controller for an existing domain

Caution: Proceeding with this option will delete all local accounts on this server.

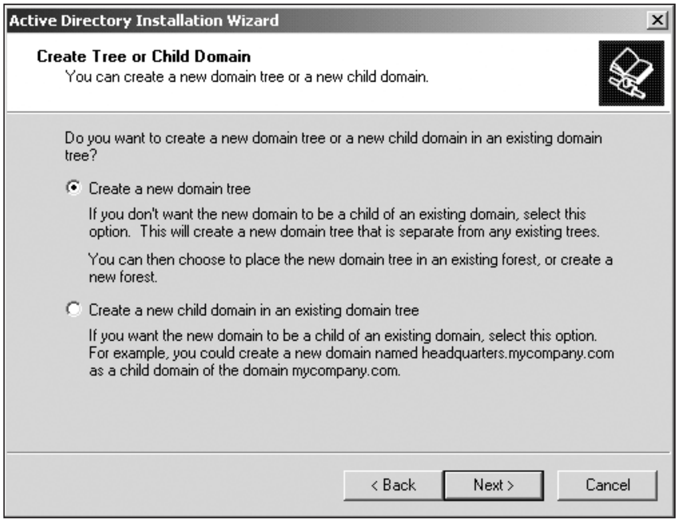
Figure 5-8 Selecting the DC role

Selecting the Domain Context

With the advent of transitive trusts in Windows 2000, the traditional NT domain structures are no longer relevant. Rather than implementing master and resource domain relationships, or creating a web of one-way and two-way trusts, domains are now structured in domain trees. As a member of a domain tree, a domain has a structured relationship with every other domain within the tree.

During the installation of a new domain, the wizard will prompt whether the new domain is a child domain within an existing domain tree, or whether the new domain forms the basis for a new domain tree. If the new domain is a child domain, you will be prompted for the placement of the domain within the tree. If you select a new tree, the wizard will assume the new domain is the root of the new tree.

For the purposes of this section, we will choose to create a new domain and new domain tree, as displayed in Figure 5-9.


Active Directory Installation Wizard

Create Tree or Child Domain
You can create a new domain tree or a new child domain.

Do you want to create a new domain tree or a new child domain in an existing domain tree?

● Create a new domain tree

If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.

You can then choose to place the new domain tree in an existing forest, or create a new forest.

○ Create a new child domain in an existing domain tree

If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.mycompany.com as a child domain of the domain mycompany.com.

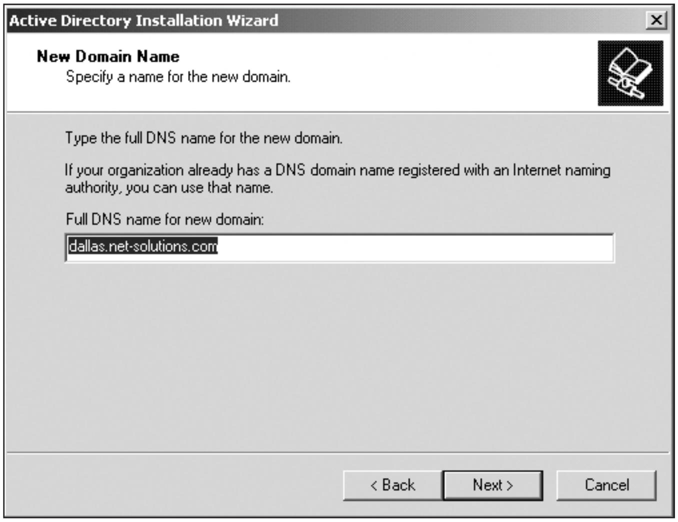
Figure 5-9 Selecting the domain context

The Domain Name

Unlike previous versions of Windows NT, Windows 2000 uses DNS rather than WINS for name resolution. One interesting effect is the need for fully qualified domain names rather than the shorter NetBIOS domain names of the past. Many times, a company will already have registered a DNS domain name for use on the Internet. If so, the internal network can be a subset, or **subdomain**, of that Internet domain name. If your company does not have a registered domain, it is best to use local as the root, to avoid name conflicts with external resources. Some companies will register two domain names and then use one for external servers and the other for internal domain structures. Doing so helps minimize the chances of internal data leaking to the outside network.

For our purposes, we will install the new domain tree for a mythical company, Net-Solutions of North Texas. Net-Solutions owns the Net-Solutions.com domain and is currently using it for external purposes only, such as maintaining a Web presence and receiving e-mail. The company's ISP currently provides DNS services for the external network. The MIS manager has decided to use the Net-Solutions.com domain name for the internal network also.

Because the company's corporate headquarters is located in Dallas, a decision is made to create a subdomain of the net-solutions.com domain and name it Dallas.Net-Solutions.com, as shown in Figure 5-10. This domain is for internal use only, and should not be registered with the external DNS server. The first server is imaginatively named Win2K, and thus the computer name is Win2k.Dallas.Net-Solutions.com.



Active Directory Installation Wizard

New Domain Name

Specify a name for the new domain.

Type the full DNS name for the new domain.

If your organization already has a DNS domain name registered with an Internet naming authority, you can use that name.

Full DNS name for new domain:

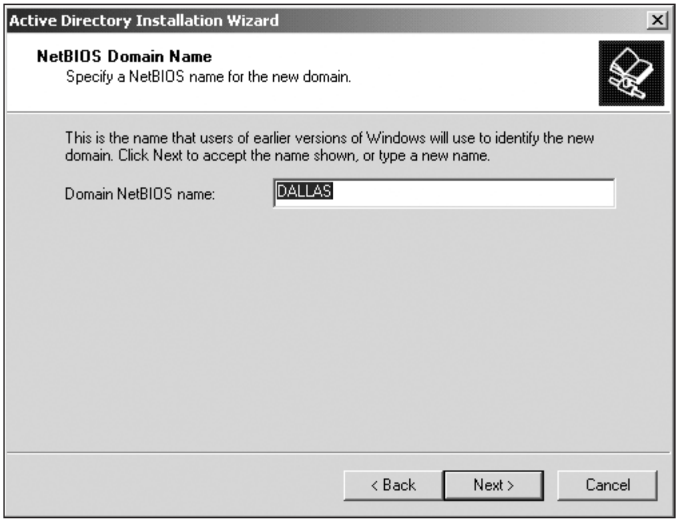
dallas.net-solutions.com

Figure 5-10 Creating the domain name

The NetBIOS Domain Name

As mentioned earlier, Windows 2000 no longer uses NetBIOS name resolution, but rather resolves names via DNS. Earlier versions of Microsoft operating systems rely on NetBIOS naming, however. These downlevel operating systems include Windows NT version 4 and previous versions, Windows 95 and 98, and Windows 3.*x*. In order for these operating systems to access a Windows 2000 domain, the domain must also be given a NetBIOS name.

In this case, we'll choose the NetBIOS domain name to match the DNS subdomain. As shown in Figure 5-11, because the DNS name of the domain is Dallas.Net-Solutions.com, the NetBIOS name of the domain is DALLAS. The domain will appear as Dallas in the domain lists when viewed by a downlevel operating system.



NetBIOS Domain Name

Specify a NetBIOS name for the new domain.

This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.

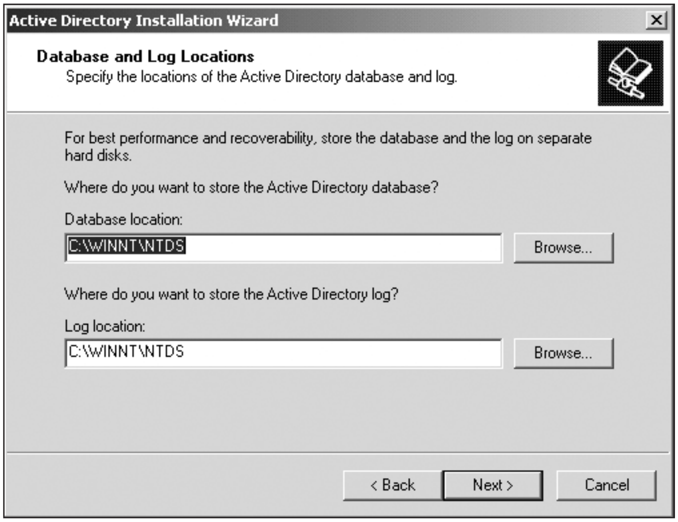
Domain NetBIOS name: DALLAS

Figure 5-11 NetBIOS domain name

Note: The NetBIOS domain name does not have to be the same as the Windows 2000 DNS domain name. However, matching the names can help ease recordkeeping and troubleshooting.

Active Directory Database and Logs

Windows 2000 uses both a database and database log files to maintain the directory within a domain. The default location for both the database and the log files is within the *%systemroot%*\NTDS directory, as seen in Figure 5-12. The **systemroot** directory is the installation location of Windows 2000; in a default Windows 2000 install, the directory will be C:\WINNT.



Active Directory Installation Wizard

Database and Log Locations

Specify the locations of the Active Directory database and log.

For best performance and recoverability, store the database and the log on separate hard disks.

Where do you want to store the Active Directory database?

Database location: C:\WINNT\NTDS

Where do you want to store the Active Directory log?

Log location: C:\WINNT\NTDS

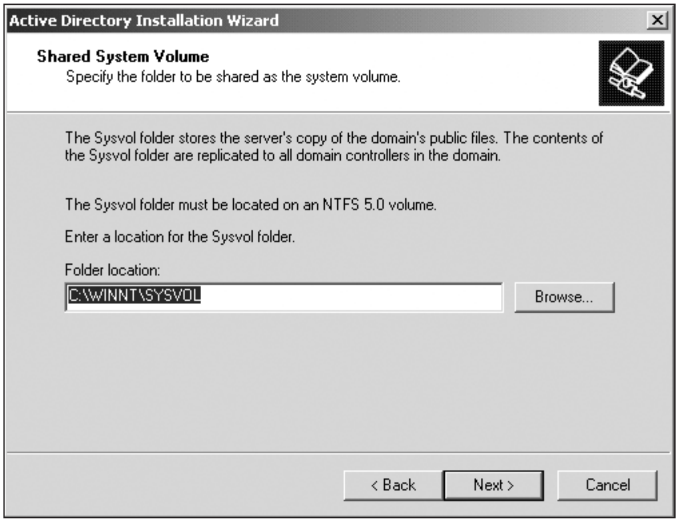
Figure 5-12 Active Directory database and logfile locations

To maximize performance on a Windows 2000 server, the log files and the database should be separated onto different physical hard drives or drive arrays. If you desire, you can split the Windows 2000 operating system, the Active Directory database, and the Active Directory log across three separate physical drives or drive arrays.

The Shared System Volume

All domain controllers within a Windows 2000 network contain a series of folders that contain the logon scripts and some policy objects for both the enterprise and the local domain. The SYSVOL share is roughly analogous to the NETLOGON share in earlier versions of the Windows NT operating systems. However, only Windows 2000 clients will read logon scripts and policies from a DC's SYSVOL share. For compatibility with downlevel systems, Windows 2000 still supports the NETLOGON share.

As shown in Figure 5-13, the default location for the shared system volume is within the *%systemroot%*\SYSVOL directory. The *systemroot* directory is the installation location of Windows 2000; in a default Windows 2000 installation, the directory will be C:\WINNT.


Active Directory Installation Wizard

Shared System Volume

Specify the folder to be shared as the system volume.

The Sysvol folder stores the server's copy of the domain's public files. The contents of the Sysvol folder are replicated to all domain controllers in the domain.

The Sysvol folder must be located on an NTFS 5.0 volume.

Enter a location for the Sysvol folder.

Folder location:

C:\WINNT\SYSVOL

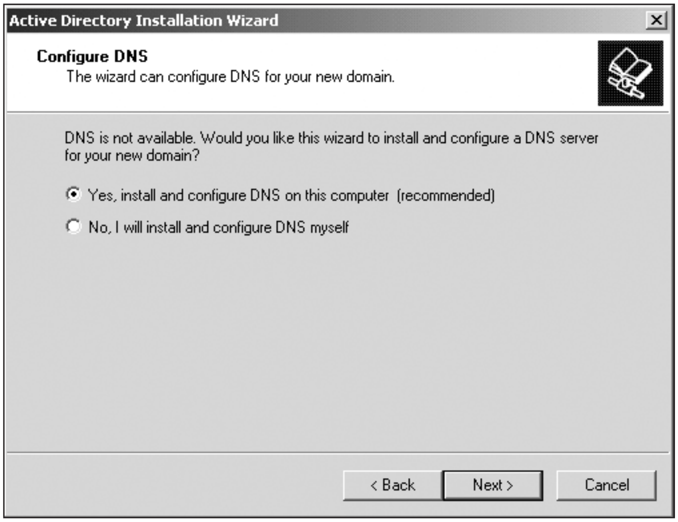
Figure 5-13 Active Directory shared system volume location

Note: The shared system volume must be located on an NTFS 5 partition or volume. NTFS 5 is the new implementation of the NT File System that is part of Windows 2000.

Installing DNS

Windows 2000 uses DNS as a method of locating the domain controllers for a domain. A client on a Windows 2000 network queries the DNS server, and the DNS server returns the address for the DC closest to the client.The client then contacts and is authorized by the DC, and uses the Active Directory database on the controller to locate objects within the domain.

Microsoft's latest implementation of DNS extends the traditional capabilities of DNS somewhat, with the integration of Dynamic Domain Name Service (DDNS). DDNS allows DCs to automatically change the records for the domain as computers join and leave the network. Due to the integration of DDNS and Active Directory, a Windows 2000 environment will require at least one server running Microsoft DNS. If the Active Directory Installation Wizard cannot communicate with a Microsoft DNS server, it will prompt you to install the DNS services, as shown in Figure 5-14.



Active Directory Installation Wizard

Configure DNS
The wizard can configure DNS for your new domain.

DNS is not available. Would you like this wizard to install and configure a DNS server for your new domain?

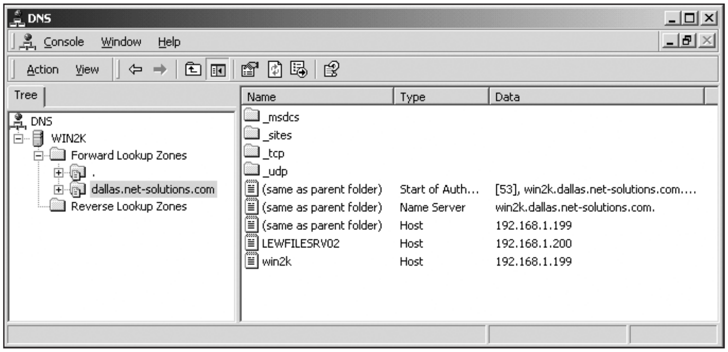
● Yes, install and configure DNS on this computer (recommended)

○ No, I will install and configure DNS myself

Figure 5-14 Installing DNS on the Windows 2000 server

If another DNS solution is already in place on the network, you need to plan carefully before activating the first Windows 2000 DNS server on the network. Failure to plan the implementation of DNS may result in incorrect name resolution for both internal network clients and external clients.

The DNS installation will automatically install the forward and reverse lookup zones for the domain and populate the zones with the Start of Authority (SOA) records, name server records, and known hosts. The default installation assumes that it is the root DNS server. DNS records can be viewed and modified via the DNS snap-in, as seen in Figure 5-15.



DNS
WIN2K
Forward Lookup Zones
.
dallas.net-solutions.com
Reverse Lookup Zones

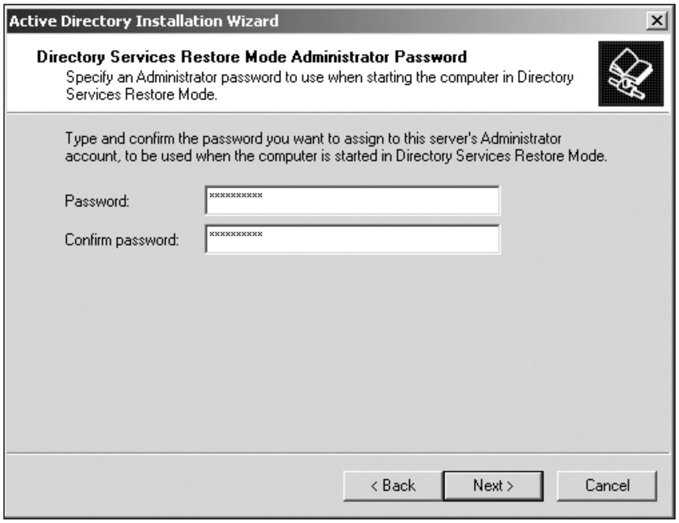
Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
(same as parent folder)	Start of Auth...	[53], win2k.dallas.net-solutions.com....
(same as parent folder)	Name Server	win2k.dallas.net-solutions.com.
(same as parent folder)	Host	192.168.1.199
LEWFILESRV02	Host	192.168.1.200
win2k	Host	192.168.1.199

Figure 5-15 Viewing DNS records on the Windows 2000 server

Directory Services Restore Mode

The Directory Services Restore Mode is a safe-mode option that allows an administrator to restore the SYSVOL directory and Active Directory database from backup if needed. The Directory Services Restore Mode requires a special local administrator logon, because the server will not be able to access the Active Directory database and thus will not be functioning as a DC in this mode.

The Restore Mode administrator account and password are similar to the local administrator role within an NT 4 member server. As seen in Figure 5-16, the Active Directory Installation Wizard will prompt for the password of the account during the installation. It is important to remember this password, because the Active Directory cannot be restored without it.



Active Directory Installation Wizard

Directory Services Restore Mode Administrator Password

Specify an Administrator password to use when starting the computer in Directory Services Restore Mode.

Type and confirm the password you want to assign to this server's Administrator account, to be used when the computer is started in Directory Services Restore Mode.

Password: ***********

Confirm password: ***********

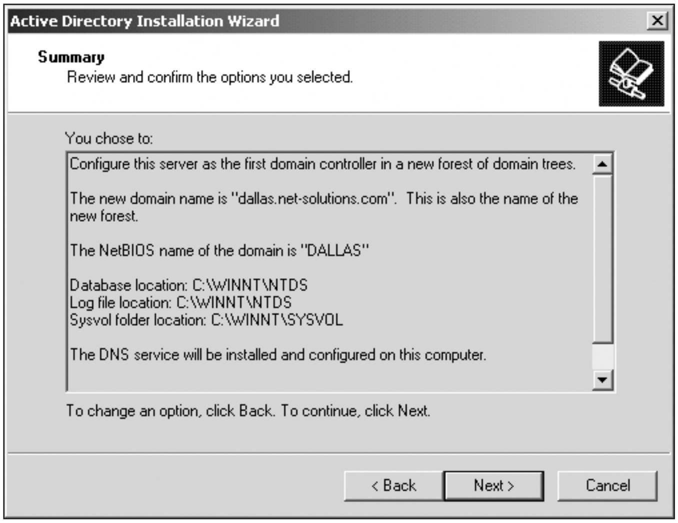
Figure 5-16 Entering the Active Directory Restore Mode password

Note

If you forget the Directory Services Restore Mode password, the Active Directory cannot be recovered on a DC. You will have to demote the server to a member server via dcpromo.exe and then reinstall Active Directory services on the server.

Final Review and Installation

After all the selections have been made, Windows 2000 will show a summary screen of your choices, as shown in Figure 5-17. If any selections need to be changed, click on the Back button to make the necessary modifications. If the selections are correct, click on Next to begin the installation of the Active Directory service and to create the Windows 2000 domain.



Summary
Review and confirm the options you selected.

You chose to:

Configure this server as the first domain controller in a new forest of domain trees.

The new domain name is "dallas.net-solutions.com". This is also the name of the new forest.

The NetBIOS name of the domain is "DALLAS"

Database location: C:\WINNT\NTDS
Log file location: C:\WINNT\NTDS
Sysvol folder location: C:\WINNT\SYSVOL

The DNS service will be installed and configured on this computer.

To change an option, click Back. To continue, click Next.

Figure 5-17 Verify final installation selections

Promoting a Server to a Domain Controller

Once a Windows 2000 domain has been created, you can add domain controllers to the domain to improve redundancy and provide additional logon points. The additional DCs contain a complete copy of the Active Directory database and replicate changes to that database to other DCs.

Windows 2000 uses a **multi-master** domain model, which means that each DC is a peer. The multi-master method provides fault tolerance by allowing any DC to process changes and updates to the Active Directory database. This process is in contrast to earlier versions of Windows NT, which required the Primary Domain Controller (PDC) to be online before modifications could be made to the domain security information.

An additional contrast to earlier versions of Windows NT is the ability to promote normal servers to DCs, and the ability to demote DCs to normal servers. Windows NT 4 and earlier required that the operating system be reinstalled if a server was to be promoted to a DC or demoted to a member server. Windows 2000 offers that ability without reinstalling the operating system.

The process of upgrading a server to a DC is similar to installing the first DC. The dcpromo.exe utility is used to promote or demote a server.

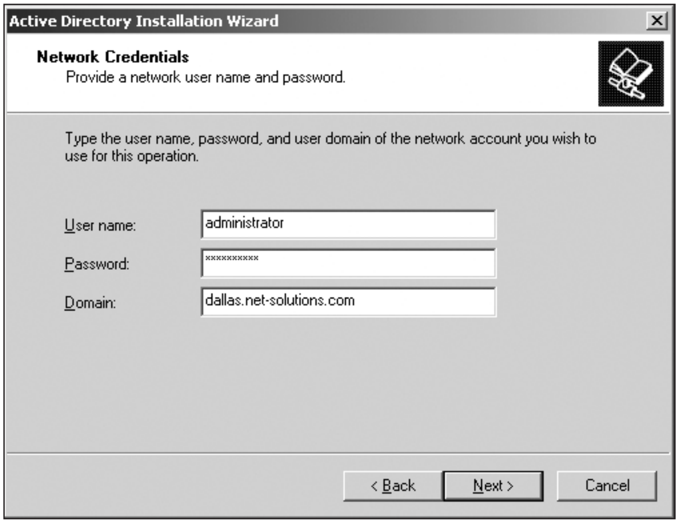
Beginning the Wizard

Start the Active Directory Installation Wizard by launching dcpromo.exe from a command line or by selecting Start|Run and entering "dcpromo.exe". Once the wizard begins, it will recognize that the server is not a DC. The wizard will give you the option of creating a new domain or adding an additional DC to a domain.

To upgrade the server to a DC within the domain, select Additional Domain Controller For An Existing Domain, as shown previously in Figure 5-4.

Network Credentials

In order to upgrade a server to a domain controller, you must have administrative rights on the server and within the domain. As shown in Figure 5-18, the wizard will prompt you for the username, password, and domain of the account you wish to use while installing the Active Directory service.



Network Credentials
Provide a network user name and password.

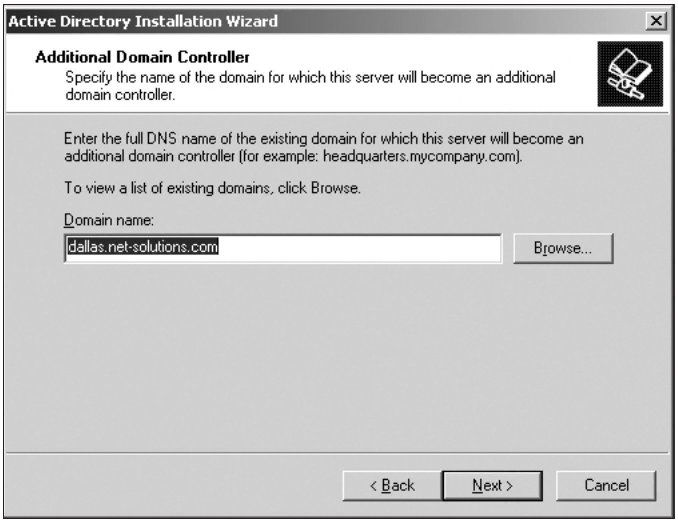
Type the user name, password, and user domain of the network account you wish to use for this operation.

User name: administrator
Password: **********
Domain: dallas.net-solutions.com

Figure 5-18 Entering the network account for the installation

Selecting the Domain

The Active Directory Installation Wizard will prompt you for the domain to which the new DC will be added. As shown in Figure 5-19, the domain name will default to the domain of which the server is currently a member. If you wish the server to become a DC within a different domain, then click on the Browse button to choose another domain.



Active Directory Installation Wizard

Additional Domain Controller

Specify the name of the domain for which this server will become an additional domain controller.

Enter the full DNS name of the existing domain for which this server will become an additional domain controller (for example: headquarters.mycompany.com).

To view a list of existing domains, click Browse.

Domain name: dallas.net-solutions.com

Figure 5-19 Selecting the domain for the new DC

The remainder of the wizard is nearly identical to the steps used in creating a new domain. You select the locations of the SYSVOL, Active Directory database, and Active Directory logs, and choose the Directory Services Restore Mode password. After that point, the directory service is installed and the domain information is replicated to the new DC. Once the database has been replicated to the server, it is ready to function as a DC on the network.

Demoting a Domain Controller

Unlike previous versions of Windows NT, Windows 2000 offers the ability to demote a domain controller to a member server without forcing an operating system reinstallation. This ability can also be used to completely remove a domain from a network.

You use dcpromo.exe to demote a DC. The program launches the Active Directory Installation Wizard. The wizard detects that the server is already a DC and offers the option to remove the Active Directory service from the server. If other DCs exist within the domain, the server will become a member server within the domain. If there are no other DCs within the domain, removing the Active Directory service will dissolve the domain and result in a standalone server.

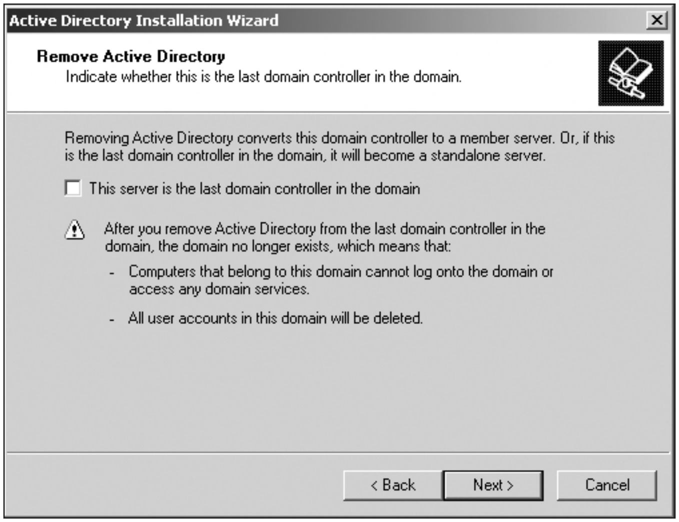
Note

Removing the last DC within a domain will result in the deletion of all domain accounts and removal of domain services. Any computers that belong to the deleted domain will be unable to log in to the domain; only local user accounts on those computers will function.

Removing Active Directory

Start the Active Directory Installation Wizard by launching dcpromo.exe from a command line or by selecting Start|Run and entering "dcpromo.exe". Once the wizard begins, it will recognize that the server is a DC. The wizard will give you the option to remove the Active Directory service and demote the server to a member server.

Select This server is the last domain controller in the domain, as shown in Figure 5-20, to remove the domain from the network and convert the server to a standalone server.



Active Directory Installation Wizard

Remove Active Directory
Indicate whether this is the last domain controller in the domain.

Removing Active Directory converts this domain controller to a member server. Or, if this is the last domain controller in the domain, it will become a standalone server.

□ This server is the last domain controller in the domain

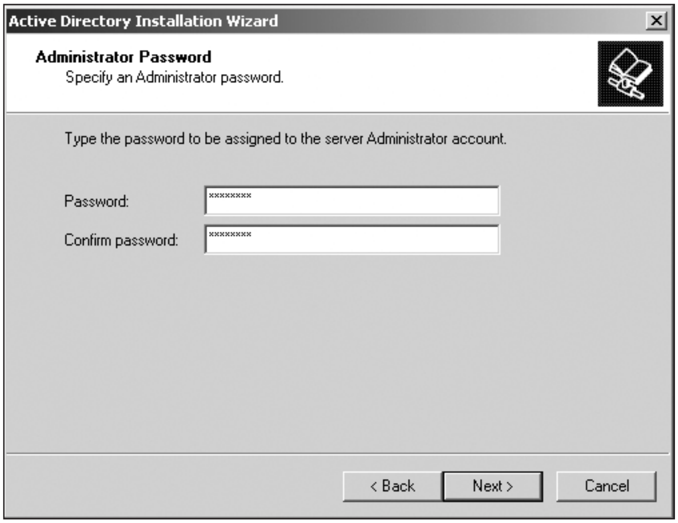
After you remove Active Directory from the last domain controller in the domain, the domain no longer exists, which means that:

- Computers that belong to this domain cannot log onto the domain or access any domain services.
- All user accounts in this domain will be deleted.

Figure 5-20 Using dcpromo.exe to remove Active Directory

Local Administrator Password

Once the Active Directory service is removed, the server will function as a member server. As with earlier versions of Windows NT, member servers have a local administrator account that applies to that particular server. The Active Directory Installation Wizard will prompt you for the password that the local administrator account should use, as shown in Figure 5-21.


Active Directory Installation Wizard
Administrator Password
Specify an Administrator password.

Type the password to be assigned to the server Administrator account.

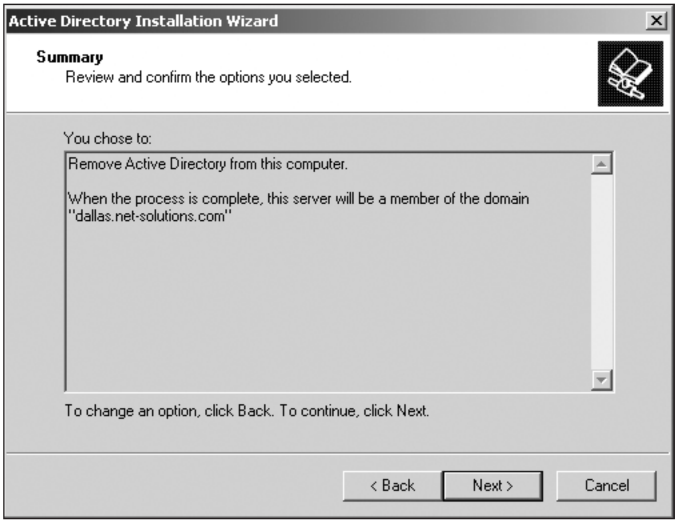
Password: *********

Confirm password: *********

Figure 5-21 Set the local administrator password

Final Review and Removal

After all the selections have been made, Windows 2000 will show a summary screen of your choices. If you need to change any selections, click on the Back button to make the necessary modifications. If the selections are correct, click on Next to begin the removal of Active Directory service. Figure 5-22 shows an example of this verification.


Active Directory Installation Wizard
Summary
Review and confirm the options you selected.

You chose to:

Remove Active Directory from this computer.

When the process is complete, this server will be a member of the domain "dallas.net-solutions.com"

To change an option, click Back. To continue, click Next.

Figure 5-22 Final verification of Active Directory removal

UNDERSTANDING THE ACTIVE DIRECTORY DATABASE

Windows 2000 uses both a database and database log files to maintain the directory within a domain. The default location for both the database and the log files is within the *%systemroot%*\NTDS directory. The *systemroot* directory is the installation location of Windows 2000; in a default Windows 2000 installation, the directory will be C:\WINNT. The database itself—the record of all the users, computers, printers, and other objects within the domain—is stored in a file named ntds.dit. This database is updated whenever an object within the domain is modified. Each of these changes is also logged, so that the database's integrity can be verified in the event the Active Directory service terminates abnormally. Both the database file and the log file are discussed in more detail in the following sections.

ntds.dit

ntds.dit is a Windows 2000 Jet database that is improved over previous versions of the Jet database engine. It is based on the same database engine used in Exchange 5.5. Two copies of the database are stored on a DC, as follows:

- *%systemroot%\NTDS\ntds.dit:* This file is the current database that is used by the DC. It contains the values for the objects within the domain and the values for the domain forest. This location can be modified during the installation of the Active Directory service.
- *%systemroot%\System32\ntds.dit:* This file is a default directory that is used by dcpromo.exe during the installation of the Active Directory service. During the installation of Active Directory, this file is copied to the location specified within the wizard. Once Active Directory is installed and started, replication from other DCs replaces the default information with the current domain information.

The ntds.dit file size will vary depending on the number of objects within the directory and the attributes associated with those objects. Each object in the directory is represented as one row in the data table, and each attribute is represented as one column in the table. Windows 2000 offers the ability to store more than 1 million objects within a directory. Microsoft has performed tests on the size of the ntds.dit file based on various numbers of objects, and has determined that most installations of Windows 2000 should not exceed 3GB of space; in fact, 500,000 user objects consumed only 1.8GB.

The size of the ntds.dit file will vary as objects are added and removed from the directory. However, the apparent size of the file will not change. This occurs because of the way NTFS reads the size of the file. NTFS records the file size when it is first opened, and will not update the size until the file is closed. Because the Active Directory service opens the ntds.dit file when the DC boots, the file size is never refreshed. You can determine the current size of the ntds.dit file in two ways:

- Reboot the DC and observe the size of the file immediately after boot.
- Use explorer.exe to determine the available space on the partition, and calculate the size of the ntds.dit file from that available space.

The ntds.dit file can be located on NTFS, FAT, or FAT32 partitions. For best results and increased redundancy, it is recommended that the database be on at least a RAID 1 (Disk Mirroring) partition.

Note

The drive containing ntds.dit must be configured for basic storage, not dynamic storage.

Database Logging

Windows 2000 Active Directory uses a log-based recovery method, in the event that the directory service is not shut down gracefully. Whenever a change is made to the directory, the change is first made dynamically within the memory of the DC, and immediately logged to the edb.log file. When the level of activity drops to an acceptable level, the changes are written permanently to the ntds.dit file and replicated across the enterprise.

If the directory service is stopped abruptly, such as in the case of a power failure, the log file is used to recover any changes that have not been written to the directory. The database reads the log files and reapplies changes in order until the database and log files are synchronized. The default location for the log file is *%systemroot%*\NTDS. This location can be changed during the installation of Active Directory. For best performance and increased redundancy, the Active Directory database and log files should be on separate partitions, and if possible separate physical drives.

Windows 2000 can either create a new log file when the current one is full, or it can overwrite the existing entries beginning with the oldest. If the system is configured to create a new log file, it is performing **noncircular logging**. If it overwrites the existing entries, it is performing **circular logging**. Circular logging saves space, but noncircular logging provides additional protection against losing database changes.

By default, Windows 2000 uses noncircular logging and creates additional files as needed. Editing the Registry can change this behavior. Modify the value of the key HKEY_LOCAL_MACHINE\CurrentControlSetServices\NTDS\Parameters\CircularLogging and set the value to 1 for circular logging or 0 (default) for non-circular logging.

Note

Registry editing should be performed with care. Incorrect modification of the Registry can result in a system that is unstable or even unbootable, and it is recommended that you have a current Emergency Repair Disk (ERD) before editing the registry.

Understanding Active Directory Domain Modes

Windows 2000 supports two modes of operation: native mode and mixed mode. A Windows 2000 domain is originally formed in a mixed mode style to provide backward compatibility with Windows NT DCs. The interoperability allows Windows NT DCs to receive replicated account updates and script or policy changes. Native mode does not support replication with Windows NT DCs, but it does allow for use of the more advanced security and grouping functions available in Windows 2000. Both mixed mode and native mode operation, including the advantages and limitations of each, are discussed in more detail in the following sections. In addition, we will discuss how to manually switch a Windows 2000 domain into native mode operation.

Mixed Mode

Mixed mode provides interoperability with domain controllers running earlier versions of Windows NT. This mode affects only the interoperability of the DCs; client computers and member servers of the domain that are running earlier versions of Windows NT or Windows 9*x* can function within a native mode domain. A network environment that has varied client or server operating systems is known as a **mixed environment**.

Mixed mode supports Security Accounts Manager (SAM) replication of both Windows 2000 and downlevel DCs such as Windows NT 4– or 3.51–based servers. A Windows 2000 domain can operate in mixed mode indefinitely, but it will not have all the capabilities of a native mode domain, such as universal groups and group nesting. Although many environments will eventually switch to native mode, there are several reasons to remain in mixed mode. Let's examine those reasons.

Inability to Upgrade Domain Controllers

In some cases, it is not feasible to upgrade a Windows NT domain controller to Windows 2000. Such cases may include unsuitable hardware for an upgrade or application incompatibilities with Windows 2000. If the DCs cannot be upgraded to Windows 2000 or cannot be downgraded to a member server, then the domain must remain in mixed mode.

Inability to Secure Domain Controllers

Due to the multimaster update method of the Active Directory service, physical security of the domain controllers is more important than ever. A physically insecure DC potentially could be used to modify accounts illicitly throughout the domain tree. If the servers cannot be secured, then leaving the DCs with a previous version of Windows NT may help minimize the potential security issues within the domain structure.

Lack of Resources to Upgrade Domain Controllers

One potential issue that is often overlooked is the cost involved in upgrading the domain controllers. In addition to any needed hardware changes, your company will have to pay Microsoft for the upgrade of the operating system. Depending on the size of the company, this may be a significant cost. Client licensing will also have to be verified with the new operating system, because some of the licensing modes have changed in Windows 2000. For some companies, any migration to Windows 2000 will have to be taken piecemeal.

Need for Fallback to Windows NT

Although proper testing will minimize any problems, there is always the possibility of problems with any new operating system. Maintaining the Windows 2000 domain as a mixed mode domain allows some degree of fallback. If it's necessary to switch back to a Windows NT–based domain, you can add a Windows NT backup DC to the domain, synchronize the SAM database, and then promote the Backup Domain Controller (BDC) to the Primary Domain Controller (PDC) of the domain. Doing so would allow for the removal of the Windows 2000 DCs without adversely affecting the clients and member servers of the domain.

Native Mode

After all DCs have been upgraded to Windows 2000, the domain can be switched to native mode. This change switches the domain from a single-master replication system to the Active Directory multi-master replication method. In addition, this change disables the NETLOGON replication, so that Windows NT DCs can no longer be added to the domain.

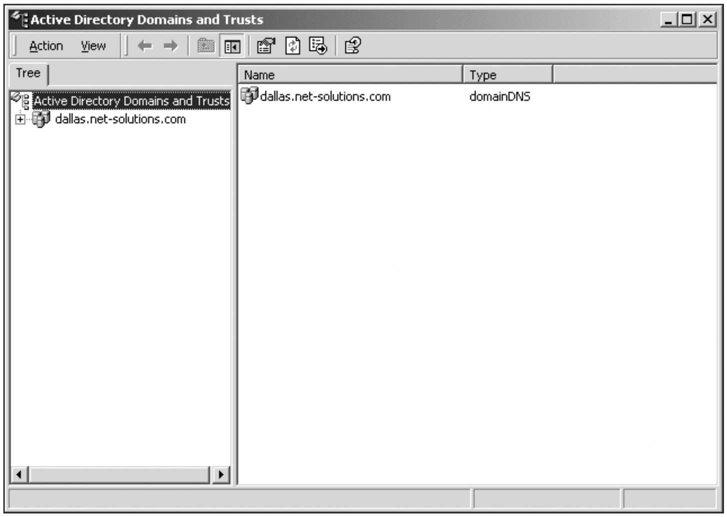
Switching to Native Mode

An administrator must manually perform the change from mixed mode to native mode. Dcpromo.exe does not have the capability to change a domain to native mode. The change is made using the administrative tools available in the Start menu or through Control Panel.

Note

The change to native mode is irreversible without the reinstallation of the OS. Once the domain has been changed to native mode, Windows NT DCs will not be able to receive account updates. Domains should not be changed to native mode if downlevel DCs are still participating in the domain.

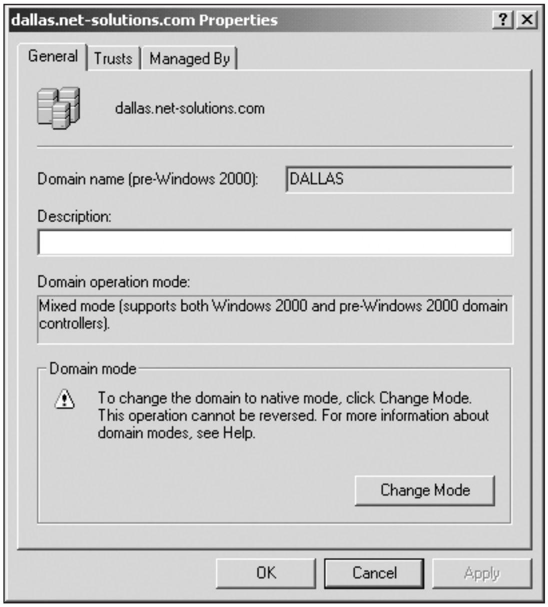
To change a domain to native mode, first open the Active Directory Domains And Trusts snap-in, as shown in Figure 5-23, and then select the domain you wish to change.


Active Directory Domains and Trusts
Action
View
Tree
Active Directory Domains and Trusts
dallas.net-solutions.com

Name	Type
dallas.net-solutions.com	domainDNS

Figure 5-23 Selecting a domain to convert to native mode

Right-click on the domain to bring up the context menu, or click on the Action menu. Select Properties for the domain. The General tab of the property sheet will show the mode in which the domain is operating. In the example shown in Figure 5-24, the domain is running in mixed mode.



Domain name (pre-Windows 2000): DALLAS

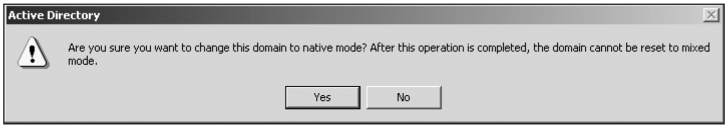
Description:

Domain operation mode:
Mixed mode (supports both Windows 2000 and pre-Windows 2000 domain controllers).

To change the domain to native mode, click Change Mode. This operation cannot be reversed. For more information about domain modes, see Help.

Figure 5-24 Domain operating in mixed mode

Click on the Change Mode button at the bottom of the General tab to switch the domain to native mode. This operation cannot be reversed. You will be prompted to verify the change before the domain is changed to native mode. Verify the change by clicking on Yes in the confirmation dialog box, as seen in Figure 5-25.

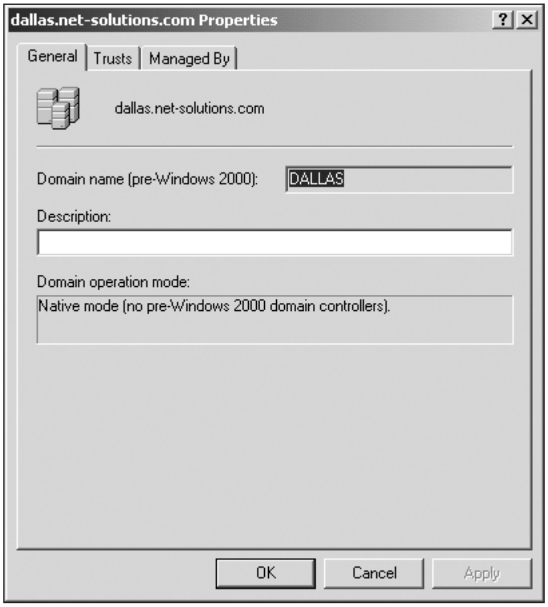


Active Directory

Are you sure you want to change this domain to native mode? After this operation is completed, the domain cannot be reset to mixed mode.

Figure 5-25 Final verification of the change to native mode

After verification, the domain will change to native mode operation. This may take some time, depending on the size of your domain and the connection speeds between your DCs. Once the domain has been changed, you can check the operational mode by again opening the property sheet of the domain. Note in Figure 5-26 that there is no longer an option to change the mode of the domain.



dallas.net-solutions.com Properties

dallas.net-solutions.com

Domain name (pre-Windows 2000): DALLAS

Description:

Domain operation mode:
Native mode (no pre-Windows 2000 domain controllers).

Figure 5-26 Domain operating in native mode

Native Mode Operation

Native mode operation modifies several aspects of the replication methods and group types. Some of the changes include:

- The domain uses Active Directory multimaster replication exclusively.
- Support for NETLOGON replication is halted.

- Windows NT DCs can no longer join the domain.
- All DCs now can perform directory updates.
- Windows 2000 group types are enabled, such as universal groups.
- Windows 2000 group nesting is now enabled.

Advantages of Native Mode Operation

The greatest advantage of native mode operation is the multi-master replication of directory changes, which allows any DC to propagate a change to the rest of the DCs within the tree. This replication is in marked contrast to the single-master method used in previous versions of Windows NT.

The second advantage to native mode operation is the automatic transitive trusts within a domain tree. With these automated transitive trusts, the administrator of the network no longer has to keep track of a web of trusts, nor is the administrator required to create the trusts manually. Instead, the Active Directory service automatically creates two-way transitive trusts when a new domain is brought into a domain tree. The result of these trusts is that users can log in to the domain from any location on the network and gain access only to their resources.

The new universal group capability is available only after a domain is operating in native mode. Additionally, all predefined security groups within Windows 2000 are available in native mode.

Chapter Summary

- Windows 2000 domains are designed around the Active Directory service, which is an enterprise-class directory service designed to provide seamless domain integration. With Active Directory, a client can log in to the network at any physical location and gain access to the correct information and resources. In addition, Active Directory automatically creates any necessary trusts between domains, freeing administrators from the manual intervention required by earlier versions of Windows NT.
- Windows 2000 uses Domain Name Service (DNS) to perform name resolution, unlike the NetBIOS name resolution of previous Microsoft operating systems. In order to provide name resolution for an ever-changing selection of client computers, Active Directory integrates closely with Dynamic Domain Name Service (DDNS). This extension of the traditional capabilities of DNS allows for dynamic updates to the DNS records as computers register themselves with the DCs. Due to this integration, a Windows 2000 domain will require at least one Microsoft DNS server within the environment.
- Windows 2000 domain structures require more planning than earlier versions of Windows NT. Because the domains are integrated within a single namespace and are automatically connected via transitive trusts, the domain space looks much like

a tree. The first domain within a Windows 2000 domain is called the root domain, and each successive domain afterwards is a child of that root domain.

- Active Directory is installed via the Active Directory Installation Wizard. This wizard can be invoked in two ways. The first method is with the Configure Your Server wizard that begins automatically after the installation of Windows 2000. The implications of this method should be considered carefully, because it also will install DHCP and DNS on the server. If these services are provided elsewhere on the network, this method should not be used, in order to avoid conflicts.

- The second method to install the Active Directory service is to use the dcpromo.exe program. This program is invoked by entering "dcpromo.exe" on the Run line of the Start menu. This method runs only the Active Directory Installation Wizard.

- You can also use dcpromo.exe to promote a member server to a DC, or to demote a DC to a member server. Unlike previous versions of Windows NT, a change in DC status does not require a reinstallation of the operating system. If the last DC in a domain is demoted, that server becomes a standalone server, and all domain accounts and services are deleted.

- The Active Directory information is stored in the ntds.dit file. This file can be located on a FAT, FAT32, or NTFS partition. The default location for this file is the *%systemroot%*\NTDS directory. This location can be modified during the Active Directory installation process. For best performance, it is recommended that this file be located on a partition that is separate from the operating system.

- Changes to the Active Directory database are logged to provide redundancy and recovery capabilities in the event that the Active Directory service is terminated abnormally. The default location for this log is the *%systemroot%*\NTDS directory. This location can be modified during the Active Directory installation process. Due to the journaling capabilities on NTFS 5, the database logs must be located on an NTFS 5 partition. The logs work in a noncircular mode by default and create new log files when the current log file is full. Modifying a Registry entry can change this behavior. The log files should be stored on a separate partition from the database files, to increase the chances of recovery in the event of a hard drive failure.

- Windows 2000 domains run in a special mode to provide interoperability with Windows NT DCs. This mode is known as mixed mode operation. Although many of the features of Windows 2000 are functional in this mode, certain capabilities—such as multi-master replication and universal groups—are not. To enable this functionality, you must switch the domain to native mode operation. This change is performed manually by the network administrator via the Active Directory Domains And Trusts snap-in. Once the domain has been switched to native mode, Windows NT DCs can no longer participate in domain security. The switch to native mode is not reversible.